Browser Extension and Login-Leak Experiment

Gábor Gulyás, Nataliia Bielova, and Claude Castelluccia

Inria, France
`http://extensions.inria.fr`

When a user browses the web, various trackers are spying on her online activities. Even though such trackers are invisible, they collect information about her, such as which pages she visits, which buttons clicks, and what text she types. This information is often used to show her targeted advertisements and may require her to pay a higher price during online shopping depending on the collected information.

Recent studies show that users can be recognised based on their device characteristics: this tracking method is called *device fingerprinting*. Such unique collection of device's properties, or a fingerprint, can often uniquely identify the user who visited the website. Usually, fingerprint includes technical parameters like what browser and operating system a visitor is using, what timezone she is from, what fonts she has in her system, or what audio card her device supports. Beyond pure technical characteristics, which are not explicitly chosen by the user, a visitor can be identified by more *behavioral* characteristics, such as the browser extensions she has installed and the websites where she has logged in. Detecting extensions and website logins can clearly make a significant contribution to fingerprinting.

In our new experiment `http://extensions.inria.fr`, we demonstrate how websites can use *behavioral fingerprinting* and detect two aspects of user's online behavior: web browser extensions and websites a user has logged in[1]. Using a detection method based on Web Accessible Resources, we are able to detect more than 13,000 Chrome browser extensions, including AdBlock, Pinterest, and Ghostery. Our experiment demonstrates an important privacy concern: the more privacy extensions you install, the more identifiable you are!

To detect the websites where a user has logged in, we use two methods: (1) redirection URL hijacking and (2) abusing Content Security Policy (CSP). We are able to successfully detect logins for 58 websites, including Gmail, Facebook, Twitter and Airbnb[2]. Detecting websites a user has logged in demonstrates another privacy problem: trackers could learn about user's preferences, when a user logs in specific shopping or dating websites, or even health-related websites.

The goal of the 5 minute talk at IEEE EuroS&P is to raise awareness about browser extension and login-leak experiment. We currently have 17,000 visitors to our website, that allows to provide a sound estimation of the visitor's identifiability based on the detected browser extensions and login-leaks.

[1] In the experiment, we collect user's browser fingerprint, together with the browser extensions installed and a list of websites the user has logged in. We only collect anonymous data during the experiment (see our Privacy Policy at `https://extensions.inrialpes.fr/privacy.php`). We securely store the data on an Inria server, use it only for research purpose and not share it with anyone outside of Inria.

[2] The list of detected browser extensions and websites can be checked here: `https://extensions.inrialpes.fr/faq.php`.